REMARKS

The Examiner's consideration of this application is sincerely appreciated. Reconsideration is respectfully requested.

Objections to Claims 9 and 26

The Office Action included objections to claims 9 and 26 which indicated the claims would be in better form if the preamble used "further comprising" instead of "wherein". Amendments to these claims have been made to make the requested changes.

Section 112 Rejections

Claims 3-5 and 20-22 were rejected under §112, ¶ 2, as being indefinite for failing to particularly point out and distinctly claim the subject mater regarded as the invention. The term "customer account information" was considered by the Examiner as not being stated and thus not providing sufficient antecedent basis for that terminology.

Claims 1 and 19 have been amended to add this terminology and thus the use thereof in claims 3-5 and 20-22 is not fully supported and this rejection is believed to be overcome.

The rejection of claim 8 as including the word "approximately" and "approximately simultaneous" has been rectified by deleting the terminology. A similar change has been made in claim 26.

The Puported Michener et al. Publication Is Not a Proper Reference

As a key matter, the Office Action cites US 2005/0010786 as a reference against this application. The date of that publication is Jan. 13, 2005. The filing date of the related application is April 1, 2002. The Applicant's filing date is May 16, 2001. Thus, the cited publication to Michener et al. ***is not a proper reference against this application.***

Although the cited publication to Michener et al. provides a purported claim to Provisional application No. 60/280,090 filed March 30, 2001; the provisional application is not being either cited or applied as the reference. The teachings contained within the provisional application are not presented, nor does the Applicant or its attorney know what is or is not contained therein.

Instead, a much later related U.S. national stage application publication is cited and applied in rejecting claims of this application. Thus, the rejections using Michener et al. are improper as based on a mistakenly applied reference which is not properly a reference under Sections 102 and 103 of the Patent Act.

In order to make out a prima facie basis for proper rejection the asserted rejection must not use as a reference a publication that is not under the Patent Law prior art. The reference thus should be retracted and should not be cited as prior art in this application.

Applicant reserves the right to argue for patentability and the inapplicability of such cited publication and the purported provisional application in this and any related application hereto.

The Carrott Patent - No. 6,839,692 Has Been Misinterpreted

Also used in rejecting claims of this application was U.S. Patent No. 6,839,692 to Carrott et al. The teachings of this reference are not sufficient to render obvious the claimed inventions. The approach used by Carrott is substantially different and teaches and leads in a direction contrary to the claimed inventions and does not render such obvious within the meaning of Section 103.

Carrott indicates that the customer codes are sent to the merchant in an encrypted form which includes the bank card numbers or other account number, social security number, name, date of birth, relative's names, address, banking information, and employment information. Column 4, lines 10-17 indicates that all of this highly sensitive information is taken and then encrypted into the "customer code". At column 5, line 60 to column 6, line 3 indicates that, "the entire customer code is populated (written to) the field on the merchant site (another embodiment of this step may include a 'rule wizard,' as discussed below). The user does not need to enter their name, address, etc. because all such information is contained in the customer code."

This approach is inherently subject to being rendered not secure, because as is well known, any code can be broken ***and the information is in fact being provided to the merchant,*** although in encoded form.

All an internet thief need do is read the encoded information and decode it. Decoding may be rendered practical or easy by using the information provided by the code confirmation site back to the merchant which decodes part of the customer code which is filled with highly sensitive information. Although this approach may work it is not equivalent to communicating without sending the sensitive information in any form whatsoever as does the Applicant's invention. Applicant teaches sending what information it does either encrypted or non-encrypted. The Carrott reference only teaches sending the information in encrypted form and the amount of type of information provided is **extremely sensitive** and yet it is stored by the merchant. Since the code confirmation site is capable of decoding, then an errant employee of such organization may abscond with decoding information and enable an internet thief to have **everything needed to abuse the customer and make fraudulent transactions of all types, not just those associated with a single account.** This is a fatal weakness, as news events have repeatedly indicated when employees that are trusted misuse or neglectfully make such identify theft information available.

Even worse, Carrott teaches sending such extremely sensitive identity-theft-enabling information is sent every time a transaction is made by the customer.

The claimed inventions are not shown nor rendered obvious by the Carrott reference. Allowance of this application is appropriate and is respectfully requested.

The Tetro Reference - Patent No. 6,095,413

The Tetro reference also does not alone or in combination with Carrott render the claimed inventions obvious. Tetro indicates that the user at a remote terminal conducting a transaction prompted to input the user's credit card information, address, and social security information. This is used for identification purposes and thus is communicated a number of times under the teachings of Tetro. Tetro indicates at column 4, lines 28-30 that the sensitive cardholder and social security information is transmitted not only by telephone, radio frequency transmission, but also by, "any other data transmission technique." This approach thus renders high sensitive personal financial information passing repeatedly for verification at a terminal.

Tetro also teaches that the sensitive financial information of the customer may be input at the vendor's store, apparently by a vendor in response to the customer giving the vendor such highly sensitive information. This is inherently ripe for abuse by the vendor or an employee of the vendor who possessed information needed to perpetrate a fraudulent transaction.

The application of Tetro in the Office Action reasons that Carrott and Michener would combine with Tetro because Tetro uses additional more sensitive information than systems that use billing address as a verification.

Tetro does not in any manner teach use of a GPS system in connection with processing a charge card transaction.

Claim 1 and Dependent Claims

The rejection of claim 1 is based upon §103(a) citing Carrott and Michener. Michener is not a proper reference as indicated above. Carrott does not in any way mention use of GPS information emanating from the ordering computer as part of a bank record for purposes of verification or authentication of a user or customer. There is not any indication suggesting such for verification. Carrott further suffers the problems indicated above in that a number of *extremely sensitive customer financial information is kept by the merchant*. The fact that the information is encoded is not an assurance that it cannot be decrypted and then abused. Carrott teaches the necessity of sending information through the merchant or directly to a code confirmation site, but in either case the merchant is always described as having the "customer code" with all this sensitive information.

Claim 1 and the related dependent claims include a limitation that the verification occurs without providing account verification information to the merchant. This is very important because it maintains the sensitive information between the bank and customer and does not impart it in any form to the merchant. This has also been added to claim 9. If the verification information is not transmitted over the internet then there is no possibility of misuse. Whereas if provided, even if encrypted, there is a risk of

disclosure. Carrott further teaches away from the invention by including many additional fields of information that are fraud enabling which may also be subject to illicit decoding and misuse.

Although Carrott mentions use of a cell phones, personal digital assistant, mobile computer or personal computer there is absolution no indication, teaching or suggestion that these devices need a GPS system, even though cell phones typically have such. Even if such devices have a GPS system it is not obvious from Carrott that GPS information is collected. Nor is there any indication that GPS information is used to verify the legitimacy of a purchase transaction. If GPS information is provided by a cell phone, the GPS location could be anywhere. Similarly, there is no teaching or suggestion that a mobile computer generates GPS information for purposes of authentication by the bank of the user or machine. Such devices are mobile. There is no indication that GPS information is used for any purpose.

The typical use of GPS information is to allow optimization of the cell phone user and the cell from which it should be connected. This has nothing to do with authentication of the purchase transaction and there is absolutely nothing suggesting such.

The Office Action indicates that Carrott fails to teach use of GPS to authenticate. Even if it was then this information is again sent along to the merchant and stored in the "customer code" and can be decoded.

Claim 1 is not obvious from Carrott and asserted and the rejection should be withdrawn. Claim 1 recites that the bank obtains ordering computer GPS information indicating that such is used to verify the ordering computer is at a position contained in the bank record for the customer. Carrott fails to teach such and it would not be obvious therefrom. Accordingly, claim 1 and dependent claims 2-3 are allowable.

Claim 4 is dependent from claim 1 and is allowable for the reasons given. It is further allowable because it recites caller identification being included in the bank record and using the telephone caller identification information for verification.

Claim 5 is further allowable in that it uses GPS information, user identification, telephone caller identification, to serve to verify the transaction is not fraudulent.

The remaining dependent claims based upon claim 1 further render the novel inventions nonobvious.

Claim 19 and Dependent Claims

Claim 19 also is nonobvious in that GPS, order delivery address are not in combination used for verifying the customer by the bank. Many of the points made above apply equally to claim 19 and dependent claims 20-35 are also allowable therewith. Other aspects of each claim also indicate the nonobviousness of the claimed methods.

With these considerations the claimed subject matter is not rendered obvious. Favorable action is appropriate and sincerely urged.

Respectfully Submitted,

Randy A. Gregory Reg. No. 30,386
GREGORY IPL CUSTOMER NO. 39279 PHONE 509.245.3033

* * * * *